Các tùy chọn bảo mật SD-WAN

Hãy cùng xem xét khả năng bảo mật SD-WAN và quan hệ hợp tác với các nhà cung cấp, bao gồm Aruba, Cisco, Riverbed và Silver Peak.

Một thành phần quan trọng của SD-WAN là khả năng bảo mật các liên kết Internet không đáng tin cậy và xác định các luồng lưu lượng bất thường, cũng như tránh các mối đe dọa từ Internet.

Các nhà cung cấp công nghệ SD-WAN đang tiếp tục tăng số lượng các tính năng bảo mật của riêng họ và tạo ra các hệ sinh thái mạnh mẽ cho các đối tác an ninh mạng.

Các nhà quản lý CNTT nên xem xét các yêu cầu bảo mật mạng nhánh của họ và đánh giá cẩn thận khả năng bảo mật của các nhà cung cấp SD-WAN hàng đầu, bao gồm các tính năng bảo mật gốc và quan hệ đối tác của họ với các nhà cung cấp bảo mật mạng.

Các mối đe dọa an ninh mạng tại các nhánh

An ninh mạng là mối quan tâm thường xuyên đối với các chuyên gia CNTT và các khảo sát cho thấy, vấn đề đang ngày càng trở nên tồi tệ hơn. Bảo mật tại các nhánh là một thách thức, do số lượng thiết bị tăng lên, bao gồm PC, máy tính bảng, điện thoại, thiết bị POS và các điểm cuối IoT, được gắn vào mạng nhánh. Tất cả các thiết bị đầu cuối này mang đến cơ hội cho các phần mềm độc hại lây nhiễm vào mạng công ty và cho tin tặc truy cập vào dữ liệu quan trọng. Các mối quan tâm về bảo mật càng trầm trọng hơn do thiếu nhân viên bảo mật/CNTT được đào tạo tại các địa điểm từ xa và sự phức tạp của việc quản lý nhiều thiết bị bảo mật bao gồm IP VPN, IDS/IPS và tường lửa.

Một thách thức nữa cho vấn đề bảo mật tại nhánh là yêu cầu phối hợp các nỗ lực bảo mật trên toàn bộ mạng. Các hệ thống bảo mật tại nhánh cần phải liên hệ trực tiếp với các sản phẩm bảo mật đầu cuối và hệ thống an ninh mạng của trung tâm dữ liệu. Lưu lượng tại nhánh cần được kiểm tra và bất kỳ lưu lượng truy cập đáng ngờ nào bị gắn cờ, tại đó có thể được phân tích bằng hệ thống bảo mật dựa trên

đám mây hoặc hệ thống bảo mật tập trung. Lý tưởng nhất là hệ thống bảo mật nhánh sẽ trở nên hoàn toàn tự động và sử dụng trí thông minh dựa trên đám mây.

Khả năng bảo mật SD-WAN

Thị trường SD-WAN có tính cạnh tranh cao với hàng chục nhà cung cấp. Một yếu tố chính khiến các doanh nghiệp muốn sử dụng SD-WAN là vì khả năng cho phép các tổ chức tận dụng các mạch Internet chi phí thấp, như các liên kết cấp doanh nghiệp an toàn. Bảo mật mạng là yếu tố mang tính phân loại chính trong công nghệ SD-WAN và mỗi nhà cung cấp có các phương pháp độc quyền của riêng mình để đảm bảo lưu lượng traffic và xác định các trang web "an toàn".

Hầu như tất cả các nhà cung cấp SD-WAN hiện nay sẽ cung cấp khả năng tường lửa cơ bản, như một tính năng sản phẩm tiêu chuẩn. Họ sử dụng nhận dạng gói để tìm hiểu lưu lượng traffic. Ví dụ, lưu lượng traffic có đến từ một vị trí tin cậy hoặc dịch vụ dựa trên đám mây hay không? Các tính năng bổ sung bao gồm lọc nội dung, xác định điểm cuối và quản lý cũng như khả năng thực thi chính sách.

Các nhà cung cấp SD-WAN đang tích cực ủng hộ các nhà cung cấp bảo mật mạng hàng đầu như Palo Alto, Z-Scaler, CheckPoint và Fortinet, để tích hợp công nghệ SD-WAN của họ với tường lửa thế hệ tiếp theo và chức năng UTM. Sự tích hợp giữa SD-WAN và các nhà cung cấp bảo mật mạng tốt nhất cần phải được sắp xếp hợp lý để đảm bảo hiệu suất cao và độ trễ thấp, vì việc chuyển giao lưu lượng giữa các ứng dụng có thể ảnh hưởng đến độ trễ. Mục tiêu là cung cấp kiểm tra lưu lượng truy cập chi tiết và lọc hiệu quả các trang web dựa trên đám mây để ưu tiên các luồng lưu lượng và ứng dụng quan trọng, an toàn.

Ví dụ về tính năng bảo mật SD-WAN

Trình quản lý chính sách của Aruba ClearPass cung cấp user, thiết bị, ứng dụng và ngữ cảnh WAN để thực thi chính sách nhất quán, thông qua giải pháp SD-WAN của nó. Việc thực thi dựa trên vai trò, điều khiển thiết bị và kiểm soát truy cập của nó, cho phép các tổ chức CNTT thực thi chính sách bảo mật mạng LAN và

WAN ở các địa điểm nhánh. Điều này giúp đơn giản hóa cách các chính sách được áp dụng trên các lớp khác nhau của mạng và giảm nhu cầu cấu hình thủ công.

RiverConnect SteelConnect hỗ trợ tường lửa chu vi tự nhiên, dịch địa chỉ mạng và phân vùng mạng, dựa trên chính sách giúp giảm thiểu xâm nhập mạng và hạn chế việc lan truyền các mối đe dọa. Nó tự động tạo các đường dẫn IPsec VPN an toàn với mã hóa AES-256 giữa các trang web và cung cấp kiểm tra kỹ càng cho các ứng dụng được mã hóa như SSL/HTTPS. SteelConnect Manager cung cấp tính năng quản lý tập trung và khả năng hiển thị, cho phép các chuyên gia CNTT chỉ định bảo mật dựa trên ứng dụng và đường dẫn lưu lượng truy cập.

Failsafe SD-WAN của Talari Networks giảm lưu lượng truy cập Internet tại nhánh, bằng cách sử dụng tường lửa tích hợp và lưu lượng truy cập URL tin cậy, có thể tự động được chuyển hướng đến Internet. Talari hỗ trợ xác thực RADIUS để truy cập quản lý các thiết bị và các gói được mã hóa của nó theo mặc định.

Ví dụ về các hệ sinh thái bảo mật SD-WAN

Một khía cạnh quan trọng của bảo mật SD-WAN là liệu các nền tảng SD-WAN có tích hợp và tương thích với các sản phẩm bảo mật mạng hàng đầu, bao gồm tường lửa nâng cao, UTM, cổng web an toàn và bảo mật mạng dựa trên đám mây hay không. Dưới đây là một số ví dụ về các hệ sinh thái bảo mật được tạo bởi các nhà cung cấp SD-WAN đã chọn.

- Cisco SD-WAN (Viptela): Giải pháp bảo mật của Cisco (đa dạng), Bluecoat, Palo Alto, Z-Scaler.
- Cloud Genix: Palo Alto, Symantec, Z-Scaler.
- Cradlepoint: Cisco, Trend Micro, Webroot, Z-Scaler.
- Silver Peak: Check point, Fortinet, Palo Alto, Z-Scaler.
- VMware (VeloCloud): Check Point, Palo Alto, Symantec, Z-Scaler.

(**Tiết lộ:** Aruba, Cisco, Cloud Genix, Cradlepoint, Riverbed, Silver Peak, Talari và VMware là các khách hàng của Doyle Research.)

SD-Branch được định nghĩa là có chức năng SD-WAN, định tuyến, bảo mật mạng và chức năng LAN/Wi-Fi, tất cả trong một nền tảng với sự quản lý tập trung và

tích hợp. Ưu điểm của SD-Branch là nó hợp nhất nhiều phần mềm/mô-đun thiết bị từ nhiều nhà cung cấp thành một nền tảng, để giúp triển khai và sử dụng dễ dàng hơn. Nhiều nhà cung cấp SD-WAN có hoặc sẽ sớm giới thiệu các giải pháp SD-Branch.

Đề xuất cho các nhà quản lý CNTT

SD-WAN là công nghệ mạnh mẽ để kết nối các tổ chức phân tán và bảo mật là điểm mấu chốt trong sự khác biệt của nhà cung cấp. Mỗi nhà cung cấp có code độc quyền cho khả năng bảo mật riêng của họ. Khách hàng nên đánh giá các công nghệ SD-WAN dựa trên cả khả năng bảo mật riêng tại nhánh và đám mây cũng như khả năng để phát triển một hệ sinh thái bảo mật mạng rộng.

Các nhà cung cấp cũng cần phải mở rộng hơn nữa và tăng cường hội nhập với một loạt các sản phẩm bảo mật mạng phổ biến, thông qua hệ sinh thái đối tác của họ.

Các nhà quản lý CNTT nên đánh giá bảo mật SD-WAN về khả năng dễ dàng tăng cường và tích hợp với môi trường bảo mật cụ thể của mình và các nhà cung cấp đương nhiệm